CASE STUDY

BrightCloud® Threat Intelligence

BrightCloud Offers Comprehensive Threat Intelligence to Innovative Security Provider, Attivo Networks

Attivo Networks adds BrightCloud® Threat Intelligence Services for URL data enrichment

At a Glance

Title
BrightCloud Offers Comprehensive Threat Intelligence to Innovative Security Provider, Attivo Networks

Vertical
Deception & Threat Detection

Founded
2011

Website
www.attivonetworks.com

Attivo Networks®, an award-winning leader in deception for cybersecurity threat detection, provides in-network threat detection. The Attivo ThreatDefend® Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds and a wide variety of specialized attack surfaces. The portfolio includes extensive network, endpoint, application, data and Active Directory deceptions designed to misdirect and reveal attacks efficiently from all threat vectors.

Attivo required a high-quality, flexible threat intelligence solution to enrich their deception-based detections informed by suspicious network traffic from their decoy environment out of the internet.

Implementing BrightCloud® Threat Intelligence Services enabled Attivo to enhance the detections from their ThreatDefend platform with data to give more contextual information about URLs and C2 servers they collected from attacker engagement with the decoys. BrightCloud provided the threat intelligence data that Attivo required to enhance their event data, providing analysts with more context on the outbound suspicious communications.

BrightCloud® Threat Intelligence Services provided Attivo with accurate, predictive and near-real-time intelligence to enhance company-centric adversary intelligence analysis and development.

BrightCloud was implemented on a flexible timeline based on Attivo's unique requirements for the marketplace.

Quick Facts:

- BrightCloud automatically adds contextual information to the Attivo URL and C2 data that would otherwise require manual research
- BrightCloud Threat Intelligence Services add key data such as geolocation and registration/WHOIS information to guide analysis and threat intelligence development
- BrightCloud Threat Intelligence Services also enhance data from the Attivo Malware Analysis Sandbox for any communications from the malware to a C2 or known malicious site

Contact us to learn more
BrightCloud.com
Phone: +1 800 870 8102

About BrightCloud

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry's most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size.